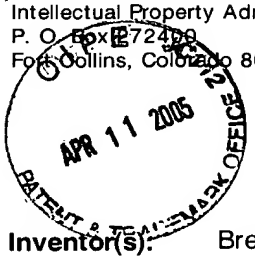
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

04/12/05

AF #

PATENT APPLICATION

ATTORNEY DOCKET NO. 10015140-1



IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Brenda P. Watlington

Confirmation No.:

Application No.: 09/896,701

Examiner: Pierre E. Elisca

Filing Date: 6/29/01

Group Art Unit: 3621

Title: CLEAR TEXT TRANSMISSION SECURITY METHOD

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on **2/11/05**.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

( )	one month	$120.00
( )	two months	$450.00
( )	three months	$1020.00
( )	four months	$1590.00

( ) The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account **08-2025** the sum of **$500.00**. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

Express Mail No. EV 570 162 539 US

(X) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit: **4/11/05**

OR

( ) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number _____ on _____

Number of pages:

Typed Name: **Andrea Blendea**

Signature: Andrea Blendea

Respectfully submitted,

Brenda P. Watlington

By _____

Roland A. Fuller III

Attorney/Agent for Applicant(s)
Reg. No. **31,160**

Date: **4/11/05**

Telephone No.: **(248) 641-1600**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application No.:	09/896,701
Filing Date:	6/29/01
Applicant:	Brenda P. Watlington
Group Art Unit:	3621
Examiner:	Pierre E. Elisca
Title:	CLEAR TEXT TRANSMISSION SECURITY METHOD
Attorney Docket:	10015140-1

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Further to the Notice of Appeal filed February 11, 2005, applicant submits this Appeal Brief.

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company L.P. An assignment was recorded in the U.S. Patent and Trademark Office on 9/30/03 at Reel/Frame: 014061/0492.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences related to the present appeal.

III. STATUS OF CLAIMS

Claims 1 - 12 are pending in this application. Claims 1 - 12 stand rejected in the Final Office Action and are the subject of this appeal. Copies of the claims on appeal are attached as Appendix A.

IV. STATUS OF AMENDMENTS

There have been no amendments submitted subsequent to the final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention relates to the way in which a data transaction terminal recognizes a data entry prompt from a remote device as a "secure prompt" in order to determine whether it is appropriate to transmit data entered into it in response to the data entry prompt as "clear text" data. More particularly, it pertains to the ability to recognize a data entry prompt as a "secure prompt" when the data entry prompt is not identical to the prompts stored in a secure prompt table. "Clear text" data, as defined in the Application, is data that is transmitted in a standard format, such as ASCII, without securing it using techniques such as encryption. [Application, p. 3, lines 15 – 18] A "secure prompt," as defined in the Application, is a data entry prompt from a remote device that prompts for the entry of non-sensitive data. [Application, p. 4, lines 17 - 19] In contrast to applicant's invention, the prior art requires that to recognize a data entry prompt as a "secure prompt," the data entry prompt must be identical to a prompt secured in a secure prompt table.

Claims 1, 2, 4, 6, 8, 10 and 12 are the independent claims. They all involve a method of determining when a data entry prompt from a remote device is a "secure

prompt" permitting transmission of data as clear text data. Claims 1, 2 and 4 are directed to a security method for transmission to a remote device of data input into a transaction terminal as clear text data, claims 6 and 8 are directed to a clear text transmission security method, and claims 10 and 12 are directed to an improved method in a data entry device of determining whether a data entry prompt is a secure prompt (claims 10 and 12).

The method is illustratively implemented in a transaction terminal having a known PIN entry device 10 (Fig. 1) and is described with reference to this known PIN entry device 10. The PIN entry device is typically linked to a remote device, such as a remote controller, such as via a network. With reference to Figs. 1 and 2, at block 102 (Fig. 2) PIN entry device 10 receives a display command from a remote controller 30 that includes a prompt (or prompt number of the prompt). At block 104, PIN entry device 10 displays the prompt on a keyboard/display 12. The display command is followed by a key string input command received at block 106 by PIN entry device 10 from remote controller 30 that directs PIN entry device 10 to wait for a string of key inputs from keypad/display 12, and upon their input, transmit them as clear text data to remote controller 30. Before accepting the key string input command, PIN entry device 10, at block 108, compares the data entry prompt received in the display command with prompts in a table of secured prompts. If the data entry prompt matches any prompt in the table of secure prompts (or the prompt number for the prompt in the table of secure prompts), or if the data entry prompt matches only a portion of any prompt in the table of secure prompts, or if any prompt in the table of secured prompts matches only a portion of the data entry prompt, PIN entry device 10 determines that the data entry prompt was a secure prompt. [Application, p. 8, line 18 – page 10, line 9]

Thus, the PIN entry device 10 determines that the data entry prompt was a secure prompt not only if it matches exactly an entry in a secure prompt table, but if there is only a partial match. In contrast, the prior art requires an exact match.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issue on appeal is:

Whether the Examiner has erred in rejecting claims 1 – 12 under 35 U.S.C. §103(a) as being unpatentable over Applicant's admitted prior art shown in Fig. 1 of the application (AAPA) and view of Caputo et al. U.S. Pat. No. 5,778,071 ("Caputo") in view of Hayosh U.S. Pat. No. 6,212,504 ("Hayosh").

VII. ARGUMENT

The Examiner Erred in Rejecting claims 1 – 12 Under 35 U.S.C. § 103(a) based on AAPA in View of Caputo.

The invention pertains to the way in which a data transaction terminal recognizes a data entry prompt from a remote device as a "secure prompt" in order to determine whether it is appropriate to transmit data entered into it in response to the data entry prompt as "clear text" data. More particularly, it pertains to the ability to recognize a data entry prompt as a "secure prompt" when the data entry prompt is not identical to the prompts stored in a secure prompt table. "Clear text" data, as defined in the Application, is data that is transmitted in a standard format, such as ASCII, without securing it using techniques such as encryption. [Application, p. 3, lines 15 - 18]

In order to prevent the interception of sensitive information, the PED Spec. imposes certain requirements on when data input into the data transaction terminal

can be transmitted as "clear text" data in response to a data entry prompt. Of pertinence here, the PED Spec. requires that data input into the data transaction terminal can be transmitted as "clear text" data only if it was input in response to a data entry prompt, calling for the entry of non-sensitive data. The Application uses the term "secure prompt" to refer to a data entry prompt that calls for the entry of non-sensitive data. In this regard, the Application expressly defines "secure prompt" "as a prompt that prompts for the entry of non-sensitive data, such as odometer readings." [Application, p. 4, lines 17 - 19]

Claims 1, 2, 4, 6, 8, 10 and 12 are the independent claims. Turning first to claim 1, claim 1 is directed to a security method for transmission to a remote device of data input into a transaction terminal as clear text data. Claim 1 recites, in pertinent part:

> "(b) determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:
>
> (i) the data entry prompt matching at least one of the prompts in the secure prompt table,
>
> (ii) the data entry prompt matching only a portion of any of the secure prompts in the secure prompts table, and
>
> (iii) any of the prompts in the secure prompt table matching only a portion of the data entry prompt."

The Examiner concedes that the AAPA does not disclose these limitations. But the Examiner takes the position that Caputo discloses "a digital algorithm (algorithm or plain text data) that includes a private/public keys [sic] or portion of the secure prompts." The Examiner then asserts that it would have been obvious to modify the teaching of AAPA with Caputo because this would prevent unauthorized access to the system using the encryption algorithm.

Applicant's invention is not directed to preventing unauthorized access to the data transaction terminal. Applicant's invention is directed to the way in which a data transaction terminal recognizes a data entry prompt from a remote device as a "secure prompt" to determine when it is appropriate to transmit data input into the data transaction terminal in response to a data entry prompt as "clear text" data.

Applicant submits that the Examiner is construing the term "secure prompt" in a manner inconsistent with its express definition in the Application and only by doing so can find that the private/public keys of Caputo are readable as "secure prompts. The Examiner does not explain why private/public keys are readable as "secure prompts." Applicant assumes that the Examiner's position is that since private/public keys deal with transmitting data in a secure fashion, they are "secure prompts." This, however, is not consistent with the definition of "secure prompts" in the Application. As discussed above, the Application defines "secure prompt" as a data entry prompt that prompts for the entry of non-sensitive data. Caputo simply does address the use of data entry prompts, let alone data entry prompts sent to a data transaction terminal to prompt for the entry of data. Caputo thus does not need to deal with determining whether a data entry prompt is a "secure prompt" or not.

Caputo, is directed to a portable security device that can be carried by an individual and connected to telephone circuits to both authenticate the individual and encrypt data communications. [Caputo, Abstract] With regard to the sections of Caputo cited by the Examiner, the first section, col. 10, lines 51 – 67, simply discloses that Caputo's data is encrypted before it is transmitted. The second section of Caputo cited by the Examiner deals with the sender of the encrypted data authenticating it and the receiver verifying it, as can be seen by the discussion in Caputo that introduces the second section cited by the Examiner. [See, Caputo et al., col. 12, lines 14 – 17]. But a

sender authenticating encrypted data and the receiver verifying it does not involve a method for transmitting data in clear text form in response to a secure prompt and does not involve determining when a data entry prompt is a secure prompt. The third section of Caputo cited by the Examiner deals with device and user authentication, i.e., digital signatures, as can be seen from the section of Caputo introducing the third section cited by the Examiner. [See, Caputo, col. 14, lines 10 - 14]. This again does not deal with transmitting data in clear text form in response to a secure prompt and does not involve determining when a data entry prompt is a secure prompt.

Moreover, using public/private keys of Caputo as "secure prompts," as the Examiner proposes, teaches away from the claimed invention. Public/private keys are inputs to algorithms that use the private key to encrypt data and the public key to decrypt the data. The exact keys must be used or the data when decrypted will be unrecognizable. As is commonly understood by those familiar with public/private keys, the exact keys must be used or the algorithms will not return valid results. Assuming that public/private keys are used as prompts, doing so would thus require that the exact keys be used. Using only part of a private key as a data entry prompt would result in a data entry prompt that would be unrecognizable when the public key is used to interpret it, and vice-versa. This is the opposite of what claim 1 requires. As discussed above, claim 1 includes limitations directed to recognizing a data entry prompt as a secure prompt when there is not exact identity between the data entry prompt and the prompts in the secure prompt table. More specifically, claim 1 includes limitations directed to recognizing a data entry prompt as a secure prompt when the data entry prompt matches only a portion of any of the secure prompts in the secure prompt table and when any of the prompts in the secure prompt table match only a portion of the data entry prompt. The Examiner has failed to show where Caputo discloses determining that a data entry

prompt is a secure prompt when only a portion of the data entry prompt matches any of the secure prompts in the secure prompt table or any of the prompts in the secure prompt table match only a portion of the data entry prompt.

Hayosh also fails to disclose the use of secure prompts, and thus cannot disclose determining that a data entry prompt is a secure prompt upon the occurrence of any of the conditions recited in claim 1, and the Examiner does not cite it as doing so. Rather, the Examiner cites Hayosh as disclosing a digital signature with clear text data. Applicant's invention is not directed to using a digital signature with clear text data, but determining whether a data entry prompt is a secure prompt and transmitting data in clear text form only upon determining that the data entry prompt is a secure prompt. Applicant submits that the combination of Hayosh with Caputo and the AAPA thus fails to disclose or suggest Applicant's invention as claimed in claim 1.

For essentially the same reasons expressed above, Applicant submits that claims 2, 4, 6, 8, 10 and 12 are allowable of the AAPA and Caputo in view of Hayosh.

For example, claim 2 recites, in pertinent part:

> "(b) determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:
>
> (i) the data entry prompt matching any prompt in the secure prompt table, and
>
> (ii) the data entry prompt matching only a portion of any prompt in the secure prompt table."

Again, the Examiner admitted that the AAPA does not disclose these limitations. Neither does Caputo or Hayosh. As discussed, Caputo does not disclose or discuss determining whether a data entry prompt is a secure prompt, and thus cannot disclose or suggest doing so based upon any of the conditions recited in claim 4. Similarly, Hayosh also

does not disclose or discuss determining whether a data entry prompt is a secure prompt. Applicant submits that claim 2 is thus allowable over the combination of the AAPA, Caputo and Hayosh.

Claim 4 recites, in pertinent part:

> "(b) determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:
>
> (i) the data entry prompt matching any prompt in the secure prompt table, and
>
> (ii) any prompt in the secure prompt table matching only a portion of the data entry prompt."

Again, the Examiner admitted that the AAPA does not disclose these limitations. Neither does Caputo or Hayosh. As discussed, Caputo does not disclose or discuss determining whether a data entry prompt is a secure prompt, and thus cannot disclose or suggest doing so based upon any of the conditions recited in claim 4. Hayosh also does not disclose or discuss determining whether a data entry prompt is a secure prompt. Applicant submits that claim 4 is thus allowable over the combination of the AAPA, Caputo and Hayosh.

The remaining independent claims, claims 6, 8, 10 and 12, contain limitations comparable to the limitations discussed above with respect to one or more of claims 1, 2 and 4. Applicant submits that claims 6, 8, 10 and 12 are thus allowable over the combination of the AAPA and Caputo in view of Hayosh.

The dependent claims, claims 3, 5, 7, 9 and 11 depend from respective ones of the independent claims and are allowable for at least that reason.

VIII. CLAIMS APPENDIX

Copies of the claims involved in this appeal, claims 1 – 12, are attached hereto as Appendix A.

Respectfully submitted,

Dated: April 11, 2005

By: _____
Roland A. Fuller III, Reg. No. 31,160

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600
RAF/akb

APPENDIX A

1. A security method for transmission to a remote device of data input into a transaction terminal as clear text data, comprising the steps of:

(a) comparing a data entry prompt for entry of data into the transaction terminal to prompts in a secure prompt table;

(b) determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i) the data entry prompt matching at least one of the prompts in the secure prompt table,

(ii) the data entry prompt matching only a portion of any of the secure prompts in the secure prompt table, and

(iii) any of the prompts in the secure prompt table matching only a portion of the data entry prompt; and

(c) transmitting the data entered into the transaction terminal in response to the data entry prompt as clear text data only upon the determination that the data entry prompt is a secure prompt.

2. A security method for transmission to a remote device of data input into a transaction terminal as clear text data, comprising the steps of:

(a) comparing a data entry prompt for entry of data into the transaction terminal to prompts in a secure prompt table;

(b) determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i) the data entry prompt matching any prompt in the secure prompt table, and

(ii) the data entry prompt matching only a portion of any prompt in the secure prompt table; and

(c) transmitting the data entered into the transaction terminal in response to the data entry prompt as clear text data only upon the determination that the data entry prompt is a secure prompt.

3. The method of claim 2, wherein the step of determining that the data entry prompt is a secure prompt includes also doing so when any prompt in the secure prompt table matches only a portion of the data entry prompt.

4. A security method for transmission to a remote device of data input into a transaction terminal as clear text data, comprising the steps of:

(a) comparing a data entry prompt for entry of data into the transaction terminal to prompts in a secure prompt table;

(b) determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i) the data entry prompt matching any prompt in the secure prompt table, and

(ii) any prompt in the secure prompt table matching only a portion of the data entry prompt; and

(c) transmitting the data entered into the transaction terminal in response to the data entry prompt as clear text data only upon the determination that the data entry prompt is a secure prompt.

5. The method of claim 4, wherein the step of determining that the data

entry prompt is a secure prompt includes also doing so when the data entry prompt matches only a portion of any prompt in the secure prompt table.

6. In a personal identification number entry device, a clear text data transmission security method, comprising the steps of:

(a) the personal identification number entry device receiving a data entry prompt for the entry of data from a remote device followed by a command from the remote device for entry of data into the personal identification number entry device;

(b) the personal identification number entry device comparing the data entry prompt to a plurality of secure prompts and determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of

(i) the data entry prompt matching any of the secure prompts, and

(ii) the data entry prompt matching only a portion of any of the secure prompts;

(c) the personal identification number entry device accepting the data entry command only upon the determination that the data entry prompt is a secure prompt.

7. The method of claim 5, wherein the step of determining that the data entry prompt is a secure prompt includes also doing so when any of the secure prompts matches only a portion of the data entry prompt.

8. In a personal identification number entry device, a clear text data transmission security method, comprising the steps of:

(a) the personal identification number entry device receiving a data entry prompt for the entry of data from a remote device followed by a command from the remote device for entry of data into the personal identification number entry device;

(b) the personal identification number device comparing the data entry prompt to a plurality of secure prompts and determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i) the data entry prompt matching any of the secure prompts, and

(ii) any of the secure prompts matching only a portion of the data entry prompt; and

(c) the personal identification number device accepting the data entry command only upon the determination that the data entry prompt is a secure prompt.

9. The method of claim 8 wherein the step of determining that the data entry prompt is a secure prompt includes also doing so when the data entry prompt matches only a portion of any of the secure prompts.

10. In a data entry device that displays a data entry prompt received from a remote device and transmits data input into the data entry device in response to the data entry prompt as clear text data only if the data entry prompt is a secure prompt, an improved method of determining whether the data entry prompt is a secure prompt, comprising the steps of:

(a) comparing the data entry prompt with prompts in a secure prompts table; and

(b) determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i) the data entry prompt matching any prompt in the secure prompt table,

(ii) the data entry prompt matching only a portion of any prompt in the secure prompt table, and

(iii) any prompt in the secure prompt table matching only a portion of the data entry prompt.

11. The method of claim 10 wherein the data entry device comprises a personal identification number entry device.

12. In a personal identification number entry device that displays a data entry prompt received from a remote device and transmits data input into the data entry device in response to the data entry prompt as clear text data only if the data entry prompt is a secure prompt, an improved method of determining whether the data entry prompt is a secure prompt, comprising the steps of:

(a) storing a plurality of secure prompts in a secure prompt table in memory of the personal identification number entry device;

(b) comparing the data entry prompt with the secure prompts stored in the secure prompt table; and

(c) determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i) the data entry prompt matching any secure prompt in the secure prompt table,

(ii) the data entry prompt matching only a portion of any secure prompt in the secure prompt table, and

(iii) any secure prompt in the secure prompt table matching only a portion of the data entry prompt.